UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/825,291	04/16/2004	Catherine Helen Gebotys	1679-14/EDEV	7948

38735 7590 07/21/2009

DIMOCK STRATTON LLP
20 QUEEN STREET WEST SUITE 3202, BOX 102
TORONTO, ON M5H 3R3
CANADA

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
07/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/825,291	GEBOTYS, CATHERINE HELEN	
	Examiner	Art Unit	
	THANHNGA B. TRUONG	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-13 and 30-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-13 and 30-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the communication filed on March 25, 2009. Claims 1-58 are pending. Claims 1-8, 14-29, and 35-58 are cancelled by the applicant. At this time, claims 9-13 and 30-34 are still rejected.

Response to Arguments

2. Applicant's arguments filed March 25, 2009 have been fully considered but they are not persuasive.

Applicant has argued that:

"Kocher does not teach or disclose the use of split masks or applying split mask values to a key as cited in claims 9-13 and 30-34."

Examiner respectfully disagrees with the applicant and still maintains that:

According to the limitation that cited in claims 9-13 and 30-34 of the instant invention, there was nothing that mentioned about splitting mask or applying split mask values to a key. Perhaps, applicant may have referred this limitation of splitting masks from set of claims in the non-elected group.

Applicant has also argued that:

"Kocher does not disclose defining a value mn as currently claimed."

Examiner respectfully disagrees with the applicant and still maintains that:

Kocher does teach the claimed subject matter of claims 9 and 30. In fact, Kocher discloses defining value of K1 and K2, similar to that of value mn as claimed, in which, Kocher shows to produce K1 and K2 from a 56-bit key K, a random value K1 is produced, then K2 is computed as K2=K XOR K1 (emphasis added). (As used herein, the term "random" shall include truly random values, as well as pseudorandom and other values that are unpredictable by an attacker. Methods for producing random values are well known in the background art and need not be described in detail here.) Next, random permutations K1P and K2P are produced, and K1P-inverse is applied to K1 and K2P-inverse is applied to K2. Similarly, to divide a message M into M1 and M2, M1 is set to equal a 64-bit random value, then M2 is set to M2=M XOR M1. Next, random permutations M1P and M2P are created and their inverses are applied to M1 and M2, respectively. The permuted keys and messages are then used, rather than the

standard key and message, during the course of cryptographic operations (column 6, lines 40-55 of Kocher).

Kocher does not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

The fact that Examiner may not have specifically responded to any particular arguments made by Applicant and Applicant's Representative, should not be construed as indicating Examiner's agreement therewith.

For the above reasons, it is believed that the rejections should be sustained

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States..

4. Claims 9-13 and 30-34 are rejected under 35 U.S.C. 102(b) as being anticipated by Kocher et al (US 6,278,783 B1).

a. *Referring to claim 9:*

i. Kocher teaches a countermeasure method for resisting security attacks on a processing unit using a key to perform a defined cryptographic function, the method comprising the following steps:

(1) obtaining the key and a random value r **(see Figure 1, element 100; column 8, line 65 through column 9, line 13 of Kocher)**;

(2) obtaining a set of n random input values m.sub.in1, ...m.sub.inn **(column 6, lines 39-45 of Kocher);**

(3) defining a masked function by masking the defined cryptographic function with the value m.sub.in1^...^m.sub.inn **(see Figure 2, element 220; column 8, lines 31-51 of Kocher);**

(4) masking the key with the random value r to define the value mkey **(see Figure 2, element 220; column 7, lines 30-33; column 8, lines 31-51 of Kocher);**

(5) obtaining a set of random values m1, . . . mn-1 **(column 6, lines 40-55; column 7, lines 30-48 of Kocher);**

(6) defining a value mn to be r^m.sub.in1^...^m.sub.inn^m1^ . . . ^mn-1 **(see Figure 2; column 7, lines 30-33; column 8, lines 31-51 of Kocher);** and

(7) using the values m1, . . . , mn and mkey to define input for the masked function **(see Figure 2, element 220; column 8, lines 31-51 of Kocher);**

b. *Referring to claim 10:*

i. Kocher further teaches:

(1) in which the encryption function is a table look-up **(column 5, lines 7-32 of Kocher).**

c. *Referring to claim 11:*

i. Kocher further teaches:

(1) in which masking is a bitwise exclusive or operation carried out on binary values **(column 2, lines 25-29 of Kocher).**

d. *Referring to claims 12-13:*

i. These claims have limitations that is similar to those of claims 9-11, thus they are rejected with the same rationale applied against claims 9-11 above.

e. *Referring to claims 30-32:*

i. This claim consists a computing device program product for resisting security attacks on a processing unit using a key to perform a defined cryptographic function, the computing device program product comprising a computer usable medium having computer readable program code means embodied in said medium to implement claims 9-11 and thus they are rejected with the same rationale applied against claims 9-11 above.

f. *Referring to claims 33-34:*

i. This claim consists a computing device program product for resisting security attacks on a processing unit using a key to perform a defined cryptographic function, the computing device program product comprising a computer usable medium having computer readable program code means embodied in said medium to implement claims 9-11 and thus they are rejected with the same rationale applied against claims 9-11 above.

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached at 571-272-3787. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2438

TBT
July 18, 2009